Claims

What is claimed:

1. A system for providing authentication over a network using a pre-established communications pipe, comprising at least one client, at least one PSD, at least one first remote computer system and at least one subsequent remote computer system,

said at least one client, further comprising;

means for transferring incoming commands sent from said first remote computer system through said pipe to said PSD,

means for transferring outgoing responses generated by said PSD to said first remote computer through said pipe, wherein said client is functionally connected to said PSD and said network and is functionally communicating over said pipe with a first remote computer system;

said at least one PSD further comprising;

at least one embedded PSD authenticating means,

means to respond to at least one incoming command,

means to generate an outgoing authentication response,

cryptography means for decrypting said incoming commands and encrypting said outgoing responses, wherein said PSD is functionally connected and is functionally communicating with said client and said first remote computer system;

said at least one first remote computer system further comprising;

means of generating outgoing commands in a proper protocol for communicating with said PSD through said pipe,

a first authenticating means for authenticating said PSD responses,

cryptography means for decrypting said incoming responses and encrypting said outgoing commands,

processing and routing means for transferring authentication challenges received over said network from said subsequent remote computer system to said PSD for authentication through said pipe,

processing and routing means for transferring authentication responses received through said pipe from said PSD to said subsequent remote computer system over said network,

wherein said first remote computer system is functionally connected to said network and is functionally communicating with said client and said PSD using said communications pipe; and

said at least one subsequent remote computer system further comprising:

means to generate authentication challenges,

a second authenticating means for authenticating responses received over said network from said PSD through said first remote computer system, wherein said second remote computer system is functionally connected to said network and is functionally communicating with said first remote computer system; and

at least one network wherein said network includes means for functionally connecting and communicating with at least one client and one or more remote computer systems.

2. A system for providing authentication over a network using a pre-established communications pipe, comprising at least one client, at least one PSD, at least one first remote computer system and at least one subsequent remote computer system,

said at least one client, further comprising;

means for transferring incoming commands sent from said first remote computer system through said pipe to said PSD,

means for transferring outgoing responses generated by said PSD to said first remote computer through said pipe.

wherein said client is functionally connected to said PSD and said network and is functionally communicating over said pipe with a first remote computer system;

said at least one PSD further comprising;

at least one embedded PSD authenticating means,

means to respond to at least one incoming command,

means to generate an outgoing authentication response,

means to transfer said authenticating means through said client to said first remote computer system,

cryptography means for decrypting said incoming commands and encrypting said outgoing responses, wherein said PSD is functionally connected and is functionally communicating with said client and said first remote computer system;

said at least one first remote computer system further comprising;

means of generating outgoing commands in a proper protocol for communicating with said PSD through said pipe,

a first authenticating means for authenticating said PSD responses,

cryptography means for decrypting said incoming responses and encrypting said outgoing commands,

storage means for storing said authenticating means transferred from said PSD,

a second authenticating means using said PSD authenticating means to provide authentication response to said subsequent remote computer system, wherein said first remote computer system is functionally connected to said network and is functionally communicating with said client and said PSD using said communications pipe; and

said at least one subsequent remote computer system further comprising:

means to generate authentication challenges,

a third authenticating means for authenticating responses received over said network from said first remote computer system, wherein said second remote computer system is functionally connected to said network and is in functional communications with said first remote computer system; and

at least one network wherein said network includes means for functionally connecting and communicating with at least one client and one or more remote computer systems.

3. The system according to claim 1 or 2 wherein said communications employs an open protocol.

4. The system according to claim 1 or 2 wherein said communications employs a secure protocol.

5. The system according to claim 1 or 2 wherein said cryptography employs asynchronous methods.

6. The system according to claim 1 or 2 wherein said cryptography employs synchronous methods.

7. A method for providing authentication over a network using a pre-established communications pipe comprising;

generating an authentication challenge on a first remote computer system in a proper format for processing by a PSD,

encrypting said properly formatted challenge using a pre-established cryptography method,

transmitting said encrypted challenge through said pipe to said PSD,

decrypting said encrypted challenge by said PSD using said pre-established cryptography method,

generating an authentication response by said PSD using said decrypted challenge and at least one internal PSD algorithm,

encrypting said authentication response using said pre-established cryptography method,

transmitting said encrypted authentication response through said pipe to said first remote computer system, and

decrypting said encrypted authentication response by said first remote computer system using said pre-established cryptography method and authenticating said response by said first remote computer system using at least one internal authentication algorithms.

8. The method according to claim 7, further comprising;

redirecting subsequent authentication challenges received over said network to said first remote computer system,

processing said subsequent authentication challenges in said proper format for processing by a PSD through said pipe,

encrypting said properly formatted challenge using said pre-established cryptography method,

transmitting said encrypted challenge through said pipe to said PSD,

decrypting said encrypted challenge by said PSD using said pre-established cryptography method,

generating an authentication response by said PSD using said decrypted challenge and at least one internal PSD algorithm,

encrypting said authentication response using said pre-established cryptography method,

transmitting said encrypted authentication response through said pipe to said first remote computer system,

decrypting said encrypted authentication response by said first remote computer system using said pre-established cryptography method, and

routing said authentication response over said network to said subsequent remote computer system, authenticating said response by said subsequent remote computer system using at least one internal authentication algorithms.

9. The method according to claim 7 wherein said communications is an open protocol.

10. The method according to claim 7 wherein said communications is a secure protocol.

11. The method according to claim 7 wherein said cryptography employs asynchronous methods.

12. The method according to claim 7 wherein said cryptography employs synchronous methods.

13. A method for providing authentication over a network using a pre-established communications pipe comprising;

generating a PSD algorithm transfer command on a first remote computer system in a proper format for processing by a PSD,

encrypting said properly formatted transfer command using a pre-established cryptography method,

transmitting said encrypted command through said pipe to said PSD,

decrypting said encrypted command by said PSD using said pre-established cryptography method,

copying said PSD algorithm into an internal memory location,

encrypting said PSD algorithm using said pre-established cryptography method,

transmitting said encrypted PSD algorithm through said pipe to said first remote computer system,

decrypting said encrypted PSD algorithm by said first remote computer system using said pre-established cryptography method and storing said PSD algorithm in a secure location,

receiving at least one remote authentication challenge over said network from at least one subsequent remote computer system by said first remote computer system,

generating an authentication response by said first remote computer system using said stored PSD algorithm,

transmitting said generated authentication response over said network to said subsequent remote computer system, and

authenticating said response by said subsequent remote computer system using at least one internal authentication algorithms.

14. The communications pipe according to claim 13 wherein said communications is an open protocol.

15. The communications pipe according to claim 13 wherein said communications is a secure protocol.

16. The cryptography according to claim 13 wherein said cryptography employs asynchronous methods.

17. The cryptography according to claim 13 wherein said cryptography employs synchronous methods.